УДК 004 **DOI: 10.18413/2518-1092-2020-5-1-0-8**

Гончаренко Ю.Ю.
Кушнарев А.А.
Лагуткина Т.В.

ИСПОЛЬЗОВАНИЕ ОБЯЗАТЕЛЬНЫХ МЕТОДОВ УСИЛЕННЫХ СРЕДСТВ ПРОГРАММНОЙ ЗАЩИТЫ ПРИ ИСПОЛЬЗОВАНИИ СЕРВИСОВ ЦИФРОВОГО ОБРАЗОВАНИЯ

Севастопольский государственный университет, ул. Университетская, д. 33, г. Севастополь, 299053, Россия

e-mail: iuliay1985@mail.ru, sahsa14.95@yandex.ru, lagutkina.tatiana@mail.ru

Аннотация
Многие фирмы и корпорации обеспокоены защитой персональных данных своих сотрудников или родственников. Потеря такой информации может повлечь финансовые проблемы или проблемы с клиентами. Однако проблемы защиты данных несовершеннолетних, волнуют немногих. Сейчас ограничивают возможность регистрации на игровых платформах для не достигших 14 или 18 лет, киносервисах, различных форумах, социальных сетях, но при этом при регистрации на образовательных платформах персональные данные могут быть обязательными для заполнения, и не защищенными от посторонних. Объем персональных данных, обрабатываемый одним государственным бюджетным учреждением, охватывает личные контактные данные минимум 700-800 учащихся, и для каждого из них одного или двух законных представителей. То есть получив доступ к одной из цифровых платформ для обучения или родительского контроля успеваемости (Дневник.ру), можно получить огромную базу данных контактов несовершеннолетних и их законных представителей для различных целей, самыми безобидными из которых является спам или реклама.
Ключевые слова: информация безопасность; персональные данные; образование; интернет; несовершеннолетние.

UDC 004

Goncharenko J.J.
Kushnaryov A.A.
Lagutkina T.V.

THE USE OF MANDATORY METHODS OF ENHANCED SOFTWARE PROTECTION IN DIGITAL EDUCATION SERVICES

Sevastopol state University, 33 Universitetskaya St., Sevastopol, 299053, Russia

e-mail: iuliay1985@mail.ru, sahsa14.95@yandex.ru, lagutkina.tatiana@mail.ru

Abstract
Many firms and corporations are concerned about the protection of the personal data of their employees or relatives. Loss of such information may result in financial or customer problems. owever, few are concerned about data protection issues for minors. Now they limit the possibility of registration on gaming platforms for those under the age of 14 or 18, cinema services, various forums, social networks, but at the same time, when registering on educational platforms, personal data can be required and not protected from strangers. The amount of personal data processed by one state budget institution covers personal contact information of at least 700-800 students, and for each of them one or two legal representatives. That is, by gaining access to one of the digital platforms for learning or parental performance monitoring (diary.ru), you can get a huge database of contacts of minors and their legal representatives for various purposes, the most harmless of which is spam or advertising.
Keywords: information; security; personal data; education; Internet; minors.

ВВЕДЕНИЕ

Персональные данные являются тем видом информации, утечка которых может привести к проблемам различного характера, при этом в большинстве случаев, очень сложно предугадать утечка какой именно информации повлечет за собой те или иные последствия [1]. Многие пользователи сети интернет не задумываясь пользуются различными сервисами, требующие при регистрации общие данные (фамилию, имя, отчество, фото, род занятий, номер телефона и т.д.), что приводит к нежелательным звонкам (реклама), увеличенному спаму на электронную почту и иное воздействие. Однако если ошибку совершил совершеннолетний гражданин, то восстановить документы, изменить номер телефона, почту, обратиться в суд он может без посторонней помощи, то при возникновении таких проблем у несовершеннолетних граждан, таким образом выйти из сложившейся ситуации не получится [2].

Целью работы является доказательство необходимости использования усиленных средств программной защиты при авторизации пользователя и обезличивания информации несовершеннолетних в процессе использования различных сервисов цифрового образования.

ОСНОВНАЯ ЧАСТЬ

Сегодня многие образовательные учреждения используют сервисы сети интернет для выдачи домашнего задания, публикации новостей, информирования родителей и законных представителей об успеваемости, но немногие сервисы обладают нужной защитой, доступ к той или иной платформе возможен только при использовании стандартного логина и пароля, что не предполагает защиту сведений содержащихся на том или ином аккаунте [3].

Утечка таких данных, как имя и фамилия, номер телефона, почта, ребенка и родителя может вызвать различные последствия, такие как звонки с угрозами, вымогательство, шантаж или иные преступные деяния.

Государственные системы, такие как автоматизированная информационная система «Зачисление», «Контингент», «Комплектование», «ЕГИССО», подразумевают подконтрольный вход в систему. В «ЕГИССО» можно получить доступ имея аккаунт руководителя государственного учреждения, а внести изменения или загрузить новые данные только имея электронно-цифровую подпись. В другие системы доступ разрешен с подготовленных и лицензируемых ФСБ персональных компьютеров, расположенных в пределах учреждения, с настроенными на них антивирусом и DLP-системой [5].

Однако, для более используемых гражданами сервисами таких требований нет, что может привести к утечке, потере, подмене информации конфиденциального характера.

Сервис «Дневник.ру» не предусматривает в своей конфигурации выбор двухфакторной авторизации (рисунок), при этом при первом входе на данный сайт нужно заполнить форму электронной почты, номера телефона, предполагает вставку фотографии, реальной даты рождения, в некоторых случаях можно заполнить поле для СНИЛСа.

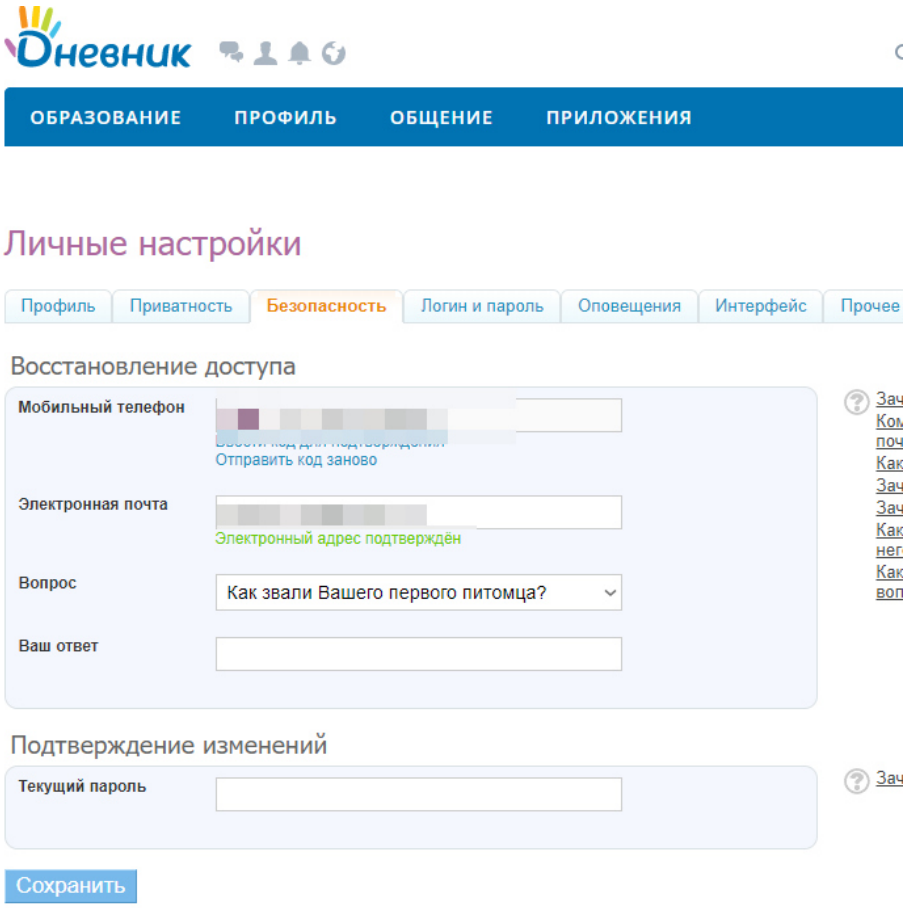

Рис. «Безопасность» профиля «Дневник.ру»
Fig. "Security" profile "Dnevnik.ru"

Если утекут данные одного-пяти пользователей образовательной организации, то решить проблему восстановления доступа и усилить пароль учащиеся смогут при помощи родителей или администрации учреждения, но если ошибку в своей работе допустит пользователь с правами Администратора, то персональные данные всех пользователей, которые заполнили формы реальными данными, будут под угрозой.

Такие платформы как «Якласс» и «Московская электронная школа» обладают более серьезной защитой.

ЯКласс – образовательная онлайн-программа для преподавателей, учеников и их родителей. Она позволяет быстро подготовиться к экзаменам и контрольным благодаря доступу к более чем 6 миллионам заданий по основным предметам средней школы. Ресурс автоматически генерирует уникальные задачи в соответствии с запросами клиента [4].

Сервис позволяет учителям создавать и проводить тесты в электронном виде, задавать домашние задания и делать процесс обучения максимально интересным и разнообразным. Ученики могут использовать систему как тренажёр для повышения знаний во всех необходимых областях, а их родители получают возможность дополнительной мотивации детей без необходимости нанимать репетитора. Разработчики указывают, что в среднем использование ресурса повышает показатель успеваемости школьников на 15%, а учителя экономят около 30% рабочего времени.

На сайте предложена обширная база бесплатных предметов, в том числе: русский язык, алгебра, геометрия и математика, физика, информатика, английский, биология, география, природоведение, химия и раздел подготовки к ЕГЭ. Учителям доступны автоматическая проверка домашних и контрольных заданий, геймификация уроков и сертификация компетенции по ИКТ. Родители могут использовать подписку «Я+», в которой отключена реклама на сайте, а также подробно написаны шаги решения задач. Также доступна статистика ребёнка в онлайн-режиме,

можно просмотреть количество сделанных заданий и общее время, которое дети провели в системе. Раздел «Переменка» содержит шуточные тесты, задачи на смекалку, логику и «вопросы замечательных людей». Кроме того, ресурс предлагает список школ с рейтингом по регионам, населённым пунктам и странам [5].

При пользовании платформой «Якласс» можно включить авторизацию, доступную при входе на почтовый сервис «Яндекс», то есть подтверждение пользователя со смартфона, ввод кода, присланного по смс или считывание QR-кода. Однако данные функции не являются обязательными, получить доступ от незащищенного аккаунта можно с помощью простого логина и пароля. А также само использование некоторых функций данной платформы является платной услугой, что ограничит использование таких функций [6].

«Московская электронная школа» является самой ограниченной по использованию платформой сетевого образования, так как доступ ко всем функциям имеют только учащиеся, педагоги и родители, имеющие отношение к московским школам. Пользователи других регионов получают доступ только к библиотеке уроков и презентаций. Доступ к платформе возможен при авторизации через почтовые сервисы, сервис «Госуслуги» и электронно-цифровую подпись. Однако данные виды доступа являются дополнительными и при получении логина и пароля пользователя остальные методы авторизации не нужны.

Основная проблема безопасности данных систем состоит в том, что подключение к этой системе в большинстве случаев, является обязательным, а также обязательным является размещение персональных данных учащихся и их законных представителей. При этом часть информации публикуется без ведома владельцев информации (это является обработкой персональных данных, согласие на которое подписывается каждым учащимся в образовательном учреждении или его законным представителем). Некоторые дополнительные данные вводят сами пользователи (для возможности восстановления доступа, для удобного использования дополнительных опций). Так, на «Дневник.ру» оформлен целый раздел, похожий на социальную сеть, где учитель или руководство школы могут публиковать новости. И дети не контролируют объем информации, который они там могут оставить, и не знают, как это может отразиться в будущем.

При этом хранение самой информации на сервере сервиса, так же необходимо настроить должным образом. Такие данные необходимо обезличивать или разделять, для того чтобы при получении доступа к серверу, нельзя было определить принадлежность данных к определенному лицу [7].

Обезличивание данных возможно несколькими способами. Можно сформировать набор персональных данных недостаточным или избыточным – убрать часть данных или добавить лишние, но убранное нельзя уничтожить – нужно его поместить в другое место, которое не будет доступно одновременно (ни на каком рабочем месте) с оставшимся набором данных. Если же информация добавлена, то в недоступное место должна быть спрятана информация об этой разнице.

В стандарте NIST SP 800-122 этот способ указан, как «разделение баз данных с использованием перекрестных ссылок». Такое разделение используется повсеместно при работе с любыми базами данных, но там не стоит задача обезличивания, поэтому базы хоть и разделены в разные хранилища, но имеют логическую связь и потому обрабатываются одновременно.

При разделении данных радикально – в одну базу выделяются все идентифицирующие реквизиты (ФИО, дата и место рождения, адрес и телефон, паспорт и т.п.) – это будет справочник физических лиц (по классификации – 3-й класс), в другой базе будет все остальное (обезличенные ПД - 4-й класс). При этом обезличенная база будет общедоступной (в т.ч. через Интернет), а база-справочник должна быть защищена от несанкционированного доступа. Утечка информации произойдет, только если злоумышленник получит базу-справочник и сможет состыковать ее с обезличенной базой. Необходимо эту возможность исключить. Но такая же стыковка нужна оператору ИСПДн для обработки ПД.

Стыковка (сопоставление) этих баз для реализации обратимости должна производиться по некому коду (идентификатору) – уникальному, но абсолютно абстрактному (нельзя использовать номера документов человека – эти реквизиты будут в справочнике). Суть стыковки состоит в сравнении идентификатора из одной базы с идентификатором другой базы – когда они одинаковы, значит, информация двух баз состыкована. Если сравнение производится на рабочем месте справочной ИСПДн, то здесь обезличенная база может быть доступна (доступность будет односторонняя, и при этом класс ИСПДн будет выше 3-го), но если сравнение производится на рабочем месте обезличенной ИСПДн, то база-справочник на этом месте недоступна, и в этом случае идентификатор из справочника может попасть в обезличенную базу только через внешний носитель. При этом внешний носитель не должен иметь реальных реквизитов того человека, код которого в нем записан. Хотя может иметь абстрактные признаки (цвет, рисунок и т.п.).

Для того, чтобы человека можно было обслуживать в рамках обезличенной базы, он должен каждый раз предъявлять этот самый внешний носитель, т.е. постоянно носить его с собой. При этом внешний носитель может иметь любую природу (бумажный, пластиковый, металлический), а абстрактные признаки носителя будут понятны только хозяину и позволят легко отличить свой носитель от чужих [8].

Таким образом, необходимо ввести обязательный модуль аутентификации, при использовании платформ, которыми пользуются несовершеннолетние граждане, так как их персональные данные не защищены должным образом. Утечка таких данных может повлечь за собой последствия для ребенка, его законных представителей, образовательного учреждения (юридическое лицо, штрафы за утечку информации в несколько раз выше, чем для гражданского лица). Предложенный способ разделения баз персональных данных позволяет обезличивать хранимую информацию с целью усиления ее безопасности.

Список литературы

1. Обработка и защита персональных данных: инструкция для владельцев сайтов URL: https://www.uplab.ru/blog/processing-and-protection-of-personal-data/ (дата обращения: 15.01.2020).
2. Персональные данные несовершеннолетних URL:https://nskdeti.nso.ru/page/1122 (дата обращения: 15.01.2020).
3. Правовая консультация: как защитить персональные данные ребенка и кто несет за это ответственность URL: https://nskdeti.nso.ru/news/1120 (дата обращения: 20.01.2020).
4. Обзор ЯКласс URL: https://coba.tools/yaklass (дата обращения: 25.01.2020).
5. Никто (почти) не знает, что такое авторизация URL: https://habr.com/ru/company/avanpost/blog/480576/ (дата обращения: 25.01.2020).
6. Введите пароль: обзор форм авторизации и альтернативных способов идентификации пользователей URL: https://vc.ru/flood/17468-authentication-state (дата обращения: 02.02.2020).
7. Двухэтапная аутентификация при использовании интернет-сервисов URL:https://www.securitylab.ru/blog/personal/bezmaly/345514.php (дата обращения: 02.02.2020).
8. Обезличивание персональных данных URL: http://www.sbchel.ru/personalnye-dannye/obezlichivanie-personalnykh-dannykh (дата обращения: 04.02.2020).

References

1. Processing and protection of personal data: instructions for site owners URL:https://www.uplab.ru/blog/processing-and-protection-of-personal-data/
2. Personal data of minors URL:https://nskdeti.nso.ru/page/1122
3. Legal advice: how to protect the personal data of the child and who is responsible for it URL:
4. Review YaKlass URL:https://coba.tools/yaklass
5. No one (almost) knows what authorization is URL:https://habr.com/en/company/avanpost/blog/480576/
6. Enter your password: an overview of authorization forms and alternative methods of user identification URL:https://vc.ru/flood/17468-authentication-state
7. Two-step authentication when using the Internet services URL:https://www.securitylab.ru/blog/personal/bezmaly/345514.php

8. Depersonalization of personal data URL: http://www.sbchel.ru/personalnye-dannye/obezlichivanie-personalnykh-dannykh

Гончаренко Юлия Юрьевна, доктор технических наук, доцент, профессор кафедры «Информационная безопасность»
Кушнарев Александр Александрович, студент второго курса магистратуры кафедры «Информационная безопасность»
Лагуткина Татьяна Владимировна, старший преподаватель кафедры «Информационные системы»

Goncharenko Julia Yurievna, Doctor of Technical Sciences, Professor of the Department "Information security"
Kushnaryov Aleksandr Alexandrovich, Second-Year Master's Student of the Department "Information security"
Lagutkina Tatiana Vladimirovna, Senior Lecturer of the Department "Information systems»